



**JPL**

*Mars Exploration Rover*

## **MER Surface Phase; Blurring the line between fault protection and what is supposed to happen**

**Glenn E. Reeves**  
**MER Flight Software Architect**  
**Jet Propulsion Laboratory**  
**California Institute of Technology**  
**[glenn.e.reeves@jpl.nasa.gov](mailto:glenn.e.reeves@jpl.nasa.gov)**



# Abstract



*Mars Exploration Rover*

- **The original, required, lifetime for the MER rovers on the surface of Mars was 90 days. Given the actual longevity of the two rovers, this small number doesn't convey the concern for efficient operation that was prevalent during the spacecraft development. A system whose reaction to each and every error or fault would require ground intervention was clearly not acceptable. Further complications included the anticipated but uncertain interaction of the rover with the Martian environment when driving or using the arm containing the contact science instruments, the constraints imposed by limitations in the vehicle hardware, and the dependence on highly coupled onboard actions (such as requiring images of the sun to establish vehicle attitude in order to properly point the antenna for communication). Many of the nominal and off-nominal scenarios required the rover software to arbitrate between competing activities or respond to errors in a limited manner such that unrelated investigations or activities could continue but the vehicle would remain safe, healthy, and able to communicate at all times. Time on the surface was an expensive resource and these challenging constraints resulted in the creation of an overall architectural design, and specific on-board behaviors, that significantly blurred the line between what was traditional fault protection and what was "normal" behavior.**
- **This paper describes how these challenges drove the system design and the resulting flight software and fault protection architecture. In many cases, behavior that would historically have been classified as fault protection became part of the expected, nominal, behavior. The paper describes how competing activities, including fault protection responses, arbitrated for authority to perform activities and how the combined system identified errors and yet limited their impact on subsequent activities. The paper includes a discussion of the most novel autonomous and semi-autonomous elements of the vehicle software including communication, surface mobility, attitude knowledge acquisition, fault protection, and the activity arbitration service. An assessment of what worked well, what did not, and the lessons that have been learned is also discussed.**

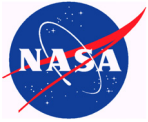


# Topics



*Mars Exploration Rover*

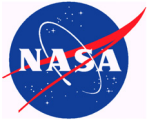
- **Requirements and Challenges**
- **MER Rover Description**
- **Chain of dependencies**
- **Implementation**



# Requirements & Challenges

*Mars Exploration Rover*

- **Mission Requirements**
  - **Land and operate solar powered rovers in the +/- 10 degree latitude band.**
  - **Operate each rover for at least 90 sols.**
  - **Utilize both X-band direct to Earth and UHF communications**
  - **Drive the rovers to at least eight separate locations and investigate geologic context and diversity.**
  - **Drive more than 600 m on at least one rover.**

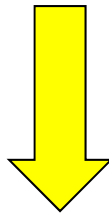


# Requirements & Challenges

*Mars Exploration Rover*

- **Mission Requirements**

- Land and operate solar powered rovers in the +/- 10 degree latitude band
- **Operate each rover for at least 90 sols**
- Utilize both X-band direct to Earth and UHF communications
- **Drive the rovers to at least eight separate locations and investigate geologic context and diversity**
- **Drive more than 600 m on at least one rover**



- **Translation**

- **Only a 90 day mission lifetime!**
  - In which to accomplish all requirements (plus hopefully more!)
- **Only 8 sites?**
  - Absolute maximum science return means optimal planning and minimum lost time
- **600 meters!**
  - Safe, semi-autonomous traverses, good distance per sol, with hazard detection

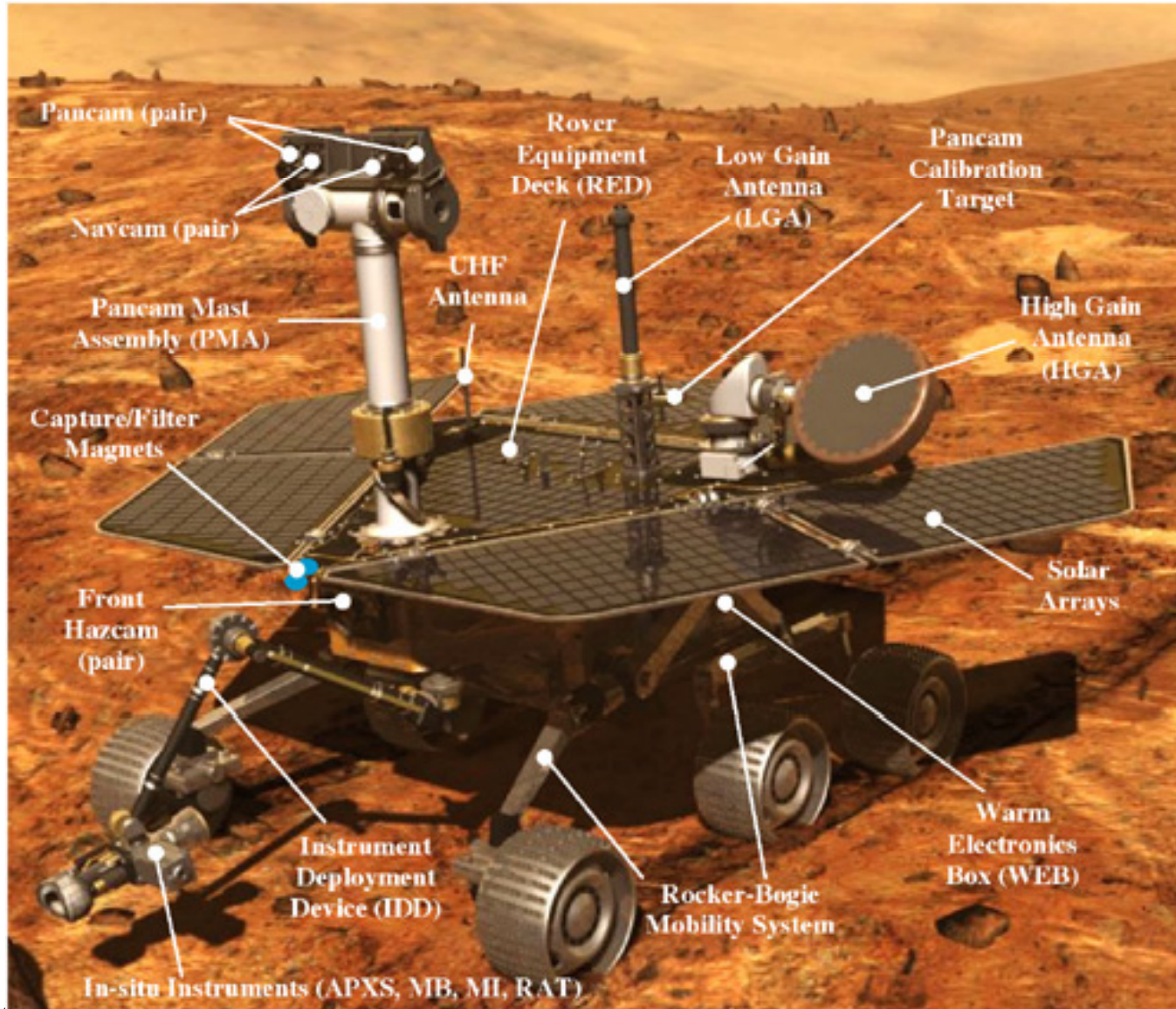


# MER Rover



**JPL**

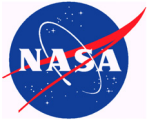
*Mars Exploration Rover*



AAS 08-052

Copyright 2008 California Institute of Technology. Government sponsorship acknowledged.

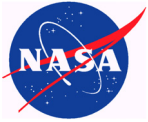
GER 6



# More Challenges and Concerns

*Mars Exploration Rover*

- **Self Imposed (Inflicted?)**
  - **Produce tactical daily plans for two rovers on Mars time**
  - **Maximize mission return**
  - **Vehicle design constraints and limitations**
- **Unknowns**
  - **In-situ interactions**
  - **Orbiter availability**
  - **Mechanism performance**



# Tactical Planning Fears

*Mars Exploration Rover*

- **The historical litany of ground responsibilities could not be accommodated in the planning time frame**
  - Opened the door to migrating responsibilities from the operations team to the flight software
- **Primary emphasis was science objectives and coordination**
  - Multiple teams, different sol “types”
- **Significant interdependence between “engineering” and “science” activities**
- **Traditional sequence model had too many products**
  - Could neither verify nor even complete all activities
- **Complicated interdependencies would require significant conservatism in activities**
  - Challenged our ability to complete mission requirements
  - Would completely eliminate the possibility of doing “better”
- **Choices in vehicle design would aggravate need for ground coordination of activities**
  - Significant number of conflicting activities would need to be coordinated manually
- **In the tactical process, science teams (multiple) and engineering teams would be defining sequence products in parallel**
  - Insufficient time in the tactical period existed for full de-conflict and prioritization



# Maximize Mission Return



*Mars Exploration Rover*

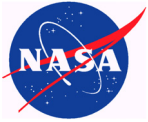
- **Inspired principal investigator**
  - Challenged team to get the most benefit during the surface mission
  - “Every moment on the surface is precious”
- **Minimum down-time**
  - No blanket “safe-mode” on errors
  - Maintain communication even in error and fault situations
  - Continuation of independent activities
    - Fault protection behavior must interact with nominal activities
  - Fast recovery of activities (operationally) demanded sufficient knowledge to avoid full sol delays
- **Oversubscription in pursuit of science**
  - Science activities planned until very end-of-day
  - Failure of primary activities initiated secondary activities



# Vehicle Design Constraints and Limitations

*Mars Exploration Rover*

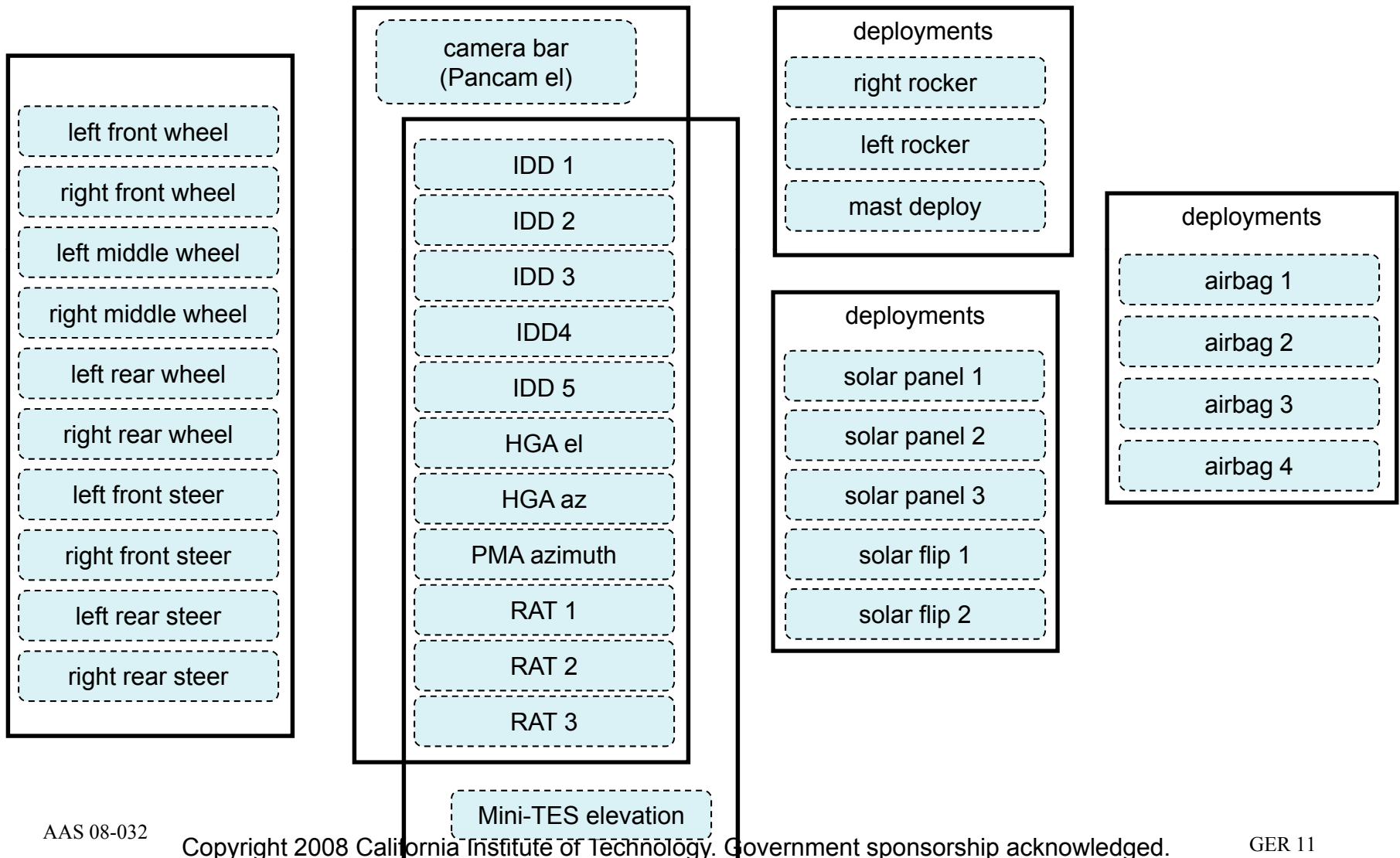
- **Design limitations**
  - **Multiplexed motor control required coordinated mechanism use**
    - **Implication: coordination of activities was necessary**
    - **Would have required excessive conservatism in activity planning to do a priori**
- **Coupled activities part of the design**
  - **Use science and engineering cameras for science, planning images , hazards, and sun identification (part of surface attitude determination)**
  - **Autonomous acquisition of attitude knowledge to ensure HGA pointing accuracy using engineering or science cameras**
- **Interference and rules**
  - **UHF and instrument use interference**
  - **Instrument/sun avoidance**
  - **Camera/instrument dust contamination**
  - **IDD stowed before driving**

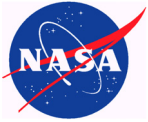


# Motor Restrictions

*Mars Exploration Rover*

Logical representation of the conflicting motor sets requiring activity arbitration:





# In-situ Uncertainty, Unknowns, Safety

*Mars Exploration Rover*

- **Both mobility and IDD us and software design need to be resilient to uncertain environment**
  - Actual performance would be unknown until Mars
- **Safety was paramount yet blanket stop and wait behavior was not desired**
  - Needed to build mechanisms that allowed both autonomous and ground control of subsequent activities in a given sol
  - Also provide restrictions on subsequent mechanical mechanism use after first error
- **Inherited mobility and IDD command model predicated on prior knowledge**
  - Vehicle motion commanded as a series of way-points
    - Starting point dependent on assumed starting position
  - IDD safety predicated on “stowed” state before vehicle motion
  - Need a mechanism to restrict activities based on coupled states and the success of prior activities



## Resulting Derived Requirements(subset)

*Mars Exploration Rover*

- **Allow simultaneous activities (to achieve mission success) without jeopardizing vehicle health and safety.**
- **Be aggressively tolerant to faults in one subsystem without affecting other, non-related subsystems.**
- **Vehicle health and safety is top priority when necessary**
- **Communication is a higher priority than science data collection or driving.**
- **Autonomously coordinate vehicle movement and communication activities so as to prevent an resource or activity conflicts**
- **The design shall allow simultaneous use of the IDD instruments, mast instrument use and pointing, the collection and processing of science data, and communication**



# Resulting Design Highlights



*Mars Exploration Rover*

- **Definition of onboard behaviors**
- **Onboard Behaviors**
  - **Communication**
  - **Surface Mobility**
  - **Surface Attitude knowledge acquisition**
  - **Activity prevention and arbitration services**
  - **Autonomous daily wakeup and shutdown**



# Resulting Design Highlights



*Mars Exploration Rover*

- “Onboard behaviors” and behavior relationships
- Onboard Behaviors
  - Communication
  - Surface Mobility
  - Surface Attitude knowledge acquisition
  - Activity prevention and arbitration services
  - Autonomous daily wakeup and shutdown



# Behavior Relationships

*Mars Exploration Rover*

- **Behaviors have identified relationship with each another based on:**
  - Resource contention
  - Health and safety issues (enforce an on-board rule)
  - Priority of activities
- **Fault protection responses are behaviors**
- **Conflicts and Resolution**
  - No conflict - allow parallel behaviors
  - Non-interacting conflict -
    - Attempting duplicate activity (i.e. commanded drive while driving)
  - Preemptive - no conflict can occur by stopping conflicting behavior prior to activity
  - Wait - lower priority granted access only after higher priority activity completes
  - Interrupting - Lower priority activity is terminated in favor of higher priority
  - Sequential - equal priorities queue for resource and are granted access in FIFO order
  - Pejorative - conflict represents a safety or rule violation
    - Future activity will also be precluded



# Communication Behavior

*Mars Exploration Rover*

- **Performs all the actions required to establish and maintain direct-to-Earth (DTE) or UHF communication with the orbiters as they**
- **pass overhead**
- **Requires no tactical planning for execution**
  - **Operations team loads several weeks worth of communication windows onboard.**
- **Windows contain all the information required to perform the communication link**
  - **start time, duration, hardware configuration, and rates**
- **HGA communication is the most complex**
  - **Several steps are required including heating and attitude knowledge acquisition**
  - **The antenna is also stowed at the end of the communication pass**



# Activity Prevention



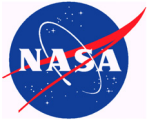
*Mars Exploration Rover*

- **Activity Constraint Manager (ACM)**
  - **Manages “permission to use” states**
  - **Precludes activities due to prior errors and due to attempts to perform activity which are disallowed given the current vehicle state**

If any condition is marked with an 'x' is true, you cannot do the activity.

You may override a condition by masking it.

Activities	If you want to	The ground didn't preclude it						No errors have occurred										The state of the vehicle is safe to do so					
	Move the vehicle	X						X	X									X	X	X		X	
	Use the Idd		X							X	X					X							X
	Use the HGA			X								X								X			
	the Camera Mast				X								X	X						X	X		
	Use the MiniTES					X							X		X					X			X
	Use the RAT						X			X	X					X	X	X					X



# Activity Coordination

*Mars Exploration Rover*

- **Arbiter (ARB)**
  - Provides activity coordination by arbitrating conflicts and granting authority to proceed
    - Enforces priorities
    - Identifies conflict and directs both conflicting behaviors
  - Manages a set of resources that can be requested by FSW “behaviors”
    - Protocol for request, grant, rescind, and cancel actions defined and embedded in FSW logic

